Hall basis of twisted Lie algebras

Marc Aubry

HALL BASIS OF TWISTED LIE ALGEBRAS

MARC AUBRY

Abstract. In this paper we define a minimal generating system for the free twisted Lie algebra. This gives a correct formulation and a proof to an old statement of Barratt. To this aim we use properties of the Lyndon words and of the Klyachko idempotent which generalize to twisted Hopf algebras some similar results well-known in the classical case.

1. Introduction

We can date the birth of twisted algebraic structures from the article of Barratt ([2]), where he proposed a new way for tackling the study of James-Hopf and Hilton-Hopf invariants. Many years later general combinatorial foundations of twisted algebraic structures were developed: elementary, combinatorial definitions by Stover ([12]) copied from the classical (non-twisted) ones; abstract, categorical definitions with the species of structures ([6], [10]). Let us also mention an operadic approach ([3], [7], [8]).

The results presented hereafter were announced in [1].

At the end of [2], Barratt gives a description of the linear basis of the free twisted Lie algebra, but without proof. Briefly, he asserts that the free twisted Lie algebra on a set of variables X is generated as a twisted module by the Lyndon words (in the classical meaning) and the brackets $[\dots[x,x]\dots,x]$, $x \in X$.

This set is minimal but it is not generating. To get a feeling of what happens, we consider the following analogy. Like free twisted Lie algebras, free graded Lie algebras satisfy $[x,x] \neq 0$ for elements x of odd degree (one can make the analogy more precise, but it is too much effort for a mere motivating example). Now look at the following graded Lie algebra: consider the graded set $X = \{x_1, x_2\}$, where the subscript represents the degree, and $L(X)$ the free graded rational Lie algebra generated by X. We quickly check that $L(X)$ admits the following basis in low dimensions:

1) In word length 1: x_1, x_2;
2) In length 2 : $[x_1,x_1], [x_1,x_2]$;
3) In length 3 : $[[x_1,x_1],x_1], [[x_1,x_2],x_2]$;
4) In length 4 : $[[[x_1,x_1],x_2],x_2], [[x_1,x_2],[x_1,x_2]]$.

Key words and phrases. Twisted Hopf algebras, twisted Lie Algebras, Klyachko idempotent, Hall basis, Dynkin word.

The element which corresponds to item 4) in the twisted case was not detected by Barratt. So we may suspect it ought to be.

We already guess how to improve Barratt's intuition. To get a generating system we have to consider the brackets $[\dots[u,u]\dots,u]$, not only for $u \in X$, but also for elements u obtained from Lyndon words: $[[x_1,x_2],[x_1,x_2]] = 2[x_1,x_2]^2$, where $[x_1,x_2]$ is obtained from the Lyndon word x_1x_2.

Our proof follows the classical one: the Lyndon words give an independant set and the Klyachko idempotent proves that this set is generating. We study the Klyachko idempotent in the Hopf algebra environment: then the proofs work abstractly on morphisms and limit the complications involved by the action of the permutation group on words.

Acknowledgements. We are indebted to F. Patras for drawing our attention to Barratt's article on twisted Lie algebras, and for pointing out that his assertion about their linear basis remains unproved. We are also grateful to the referee who incited us to clarify various notions of freeness for twisted objects.

The paper is organized as follows.

We recall some definitions about twisted algebraic structures very briefly in Section 2. We also set up notations once for all.

Section 3 gives a short account on various notions of free twisted associative and Lie algebras. Some light is brought to associative and Lie polynomials in the twisted case.

In section 4, we discuss Lyndon words and prove the minimality of our Hall basis.

Section 5 proves the properties of the Klyachko idempotent for Hopf algebras.

In Section 6 we prove that our basis is generating.

2. Twisted algebras

We briefly review some twisted algebraic structures we shall use in the following sections. A complete exposition was given by Stover ([12]). We follow his presentation : it is very explicit on elements and so immediately manageable when we construct Hall basis.

First we fix some notation for the permutation group.

2.1. **Permutation groups.**

Let us denote by $\mathfrak{S}_n$ the group of all bijections of n objects; in the following it is understood (if the converse is not specified) that these objects are the set of integers $\{1,\dots,n\}$; we also explicitely denote a permutation σ by its image $(\sigma(1),\dots\sigma(n))$. We compose permutations as usual for maps by acting on the left $\sigma\circ\tau(i)=\sigma(\tau(i))$.

Given a decomposition (all integers in the following are non-negative) (p_1,p_2) of $n=p_1+p_2$ (by abuse we shall say a decomposition $n=p_1+p_2$), we define the inclusion $\mathfrak{S}_{p_1} \times \mathfrak{S}_{p_2} \subset \mathfrak{S}_n$ as reflecting the inclusion given on objects by the map preserving order from left to right:

$$\{1, \dots, p_1\} \coprod \{1, \dots, p_2\} \subset \{1, \dots, n\}$$
$$i \mapsto i \text{ on the first factor}$$
$$i \mapsto p_1 + i \text{ on the second factor}$$

(As above and by abuse, for $\coprod$ order matters). One immediately extends this to the case $n = p_1 + \cdots + p_k$, $k \geq 2$, to define $\mathfrak{S}_{p_1} \times \cdots \times \mathfrak{S}_{p_k} \subset \mathfrak{S}_n$. If Φ_i are permutations in $\mathfrak{S}_i$ we denote then by $(\Phi_1, \dots, \Phi_k)$ the image in $\mathfrak{S}_n$ of $(\Phi_1 \times \cdots \times \Phi_k) \in \mathfrak{S}_{p_1} \times \cdots \times \mathfrak{S}_{p_k}$.

We now define permutations acting on blocks. Let $n = p_1 + \cdots + p_k$ be some decomposition and $\sigma \in \mathfrak{S}_k$. We define the permutation of $\mathfrak{S}_n$ acting on the k-blocks $p_1, \dots, p_k$ by the following composition:

$$\mathcal{C}_{p_{\sigma^{-1}(1)}, \dots p_{\sigma^{-1}(k)}}(\sigma) : \{1, \dots, n\} \to \{1, \dots, p_1\} \coprod \cdots \coprod \{1, \dots, p_k\}$$
$$\to \{1, \dots, p_{\sigma^{-1}(1)}\} \coprod \cdots \coprod \{1, \dots, p_{\sigma^{-1}(k)}\} \to \{1, \dots, n\}$$

where the first and last arrows preserve the order from left to right, and the second one preserves the elements (i.e. if $\sigma(j) = i$, at the l-th spot of the i-th block of the image you find the element that was at the l-th spot of the j-th block in the preimage).

We also recall the following

Proposition 2.1.1. 1) *For all $\sigma, \tau \in \mathfrak{S}_k$, we have*

$$\mathcal{C}_{p_{(\sigma\circ\tau)^{-1}(1)}, \dots, p_{(\sigma\circ\tau)^{-1}(k)}}(\sigma\circ\tau) = \mathcal{C}_{p_{(\sigma\circ\tau)^{-1}(1)}, \dots, p_{(\sigma\circ\tau)^{-1}(k)}}(\sigma)\circ\mathcal{C}_{p_{\tau^{-1}(1)}, \dots, p_{\tau^{-1}(k)}}(\tau).$$

2) *For all $\sigma \in \mathfrak{S}_k$, $\Phi_1 \in \mathfrak{S}_{p_1}$, $\dots$, $\Phi_k \in \mathfrak{S}_{p_k}$, we have*

$$\mathcal{C}_{p_{\sigma^{-1}(1)}, \dots, p_{\sigma^{-1}(k)}}(\sigma)\circ(\Phi_1\times\cdots\times\Phi_k) = (\Phi_{\sigma^{-1}(1)}\times\cdots\times\Phi_{\sigma^{-1}(k)}) \circ \mathcal{C}_{p_{\sigma^{-1}(1)}, \dots, p_{\sigma^{-1}(k)}}(\sigma).$$

2.2. **Twisted modules and tensor products.** Let R be a ring. A graded R-module X is a collection $(X_n)_{n\in\mathbb{N}}$ of R-modules X_n indexed by the non-negative integers.

Twisted modules. A twisted module M is a graded module together with a right $\mathfrak{S}_n$-action (a right $R(\mathfrak{S}_n)$-module structure on X_n for each n). Morphisms of graded R-modules and of twisted modules are defined as one can imagine; we shall only consider morphisms of degree 0. A twisted module M is connected if $M_0 = 0$. R is canonically given a structure of twisted module.

Twisted tensor product. The twisted tensor product of k twisted modules $M_1, \dots, M_k$ is defined by its nth-term

$$(M_1\otimes\cdots\otimes M_k)_n = \sum_{\substack{p_1 + \cdots + p_k = n \\ p_i \geq 0}} ((M_1)_{p_1}\otimes_R\cdots\otimes_R(M_k)_{p_k})\otimes_{R(\mathfrak{S}_{p_1}\times\dots\mathfrak{S}_{p_k})}R(\mathfrak{S}_n).$$

2.3. **Twisted algebras and coalgebras.** With the definitions given above, we can formally define twisted algebras and twisted coalgebras by the same diagrams we do for the classical cases.

Like the classical case again we define the tensor twisted algebra $A \otimes B$ of two twisted algebras A and B, the product of which is the composition

$$A \otimes B \otimes A \otimes B \xrightarrow{A \otimes T \otimes B} A \otimes A \otimes B \otimes B \xrightarrow{\mu_A \otimes \mu_B} A \otimes B$$

which we can explicit on elements

$$((a_1 \otimes b_1) \circ \sigma_1)((a_2 \otimes b_2) \circ \sigma_2) = ((a_1 a_2) \otimes (b_1 b_2) \circ \mathcal{C}_{p_1,p_2,q_1,q_2}(T) \circ (\sigma_1 \times \sigma_2).$$

We have denoted by T the swap $A \otimes B \to B \otimes A$ and by σ the permutation $(1, 3, 2, 4)$.

2.4. **Twisted bialgebras, Hopf algebras.** We refer to [12] for the definitions of twisted algebras, coalgebras and bialgebras. Formally they reproduce the definition diagrams of the classical case.

Definition 2.4.1. A twisted bialgebra is a twisted module A, which is both a twisted algebra with product $\mu : A \otimes A \to A$ and unit $\epsilon : R \to A$ and coalgebra with coproduct $\Delta : A \to A \otimes A$ and counit $\eta : A \to R$, such that both μ and η are morphisms of twisted coalgebras or, equivalently both Δ and ϵ are morphisms of twisted algebras; here $A \otimes A$ is given the structure of twisted coalgebra (resp. algebra) induced by A and depicted in the preceding subsection.

Let us just emphasize the existence of the antipode in the axioms of Hopf algebras.

Definition 2.4.2. A twisted Hopf algebra is a twisted bialgebra A together with a morphism of twisted modules $S : A \to A$ such that the following diagram commutes:

$$\begin{tikzcd}
A \arrow[r, "\Delta"] \arrow[dd, "\Delta"'] \arrow[dr, "\eta"] & A \otimes A \arrow[r, "S \otimes A"] & A \otimes A \arrow[dd, "\mu"] \\
& R \arrow[dr, "\epsilon"] & \\
A \otimes A \arrow[r, "A \otimes S"] & A \otimes A \arrow[r, "\mu"] & A
\end{tikzcd}$$

where $\eta : A \to R$ (resp. $\epsilon : R \to A$) is the counit (resp. unit) of the coalgebra (resp. algebra) A.

Convolution. At this point it seems judicious to introduce an operation we shall use very often in the next sections.

Proposition 2.4.3. *Let C be a twisted coalgebra and A be a twisted algebra. The set of morphisms of twisted modules $Hom_{R(\mathfrak{S})}(C,A)$ is an associative monoid with the following product, called the convolution and denoted by $\star$:*

$$f \star g : C \xrightarrow{\Delta} C \otimes C \xrightarrow{f \otimes g} A \otimes A \xrightarrow{\mu} A$$

Now, by definition the antipode is the inverse of the identity under the convolution product; it is thus unique. Like the classical case there is a canonical way to define an antipode on a twisted connected bialgebra and thus to give it the structure of a twisted Hopf algebra.

Before continuing our description of twisted algebraic structures, let us recall the notion of pseudo-coproduct in cocommutative twisted bialgebras. We shall need it for the Klyachko idempotent (Section 5) and we reffered already toit for the Dynkin idempotent in [1].

Let A be a cocommutative bialgebra. We use notations of Section 2 and denote by π, Δ, η and ϵ respectively its product, coproduct, unit and counit. Let $\nu = \eta \circ \epsilon$. Formally the same definition as in [9] works.

Definition 2.4.4. An endomorphism f of A (here and in the sequel endomorphism means $\mathbb{F}(\mathfrak{S})$-module endomorphism, and we denote the corresponding set - $\mathbb{F}$-module - by $\mathrm{End}(A)$) admits $F \in \mathrm{End}(A \otimes A)$ as a pseudo-coproduct if $F \circ \Delta = \Delta \circ f$. If f admits the pseudocoproduct $f \otimes \nu + \nu \otimes f$, we say that f is pseudo-primitive.

2.5. **Lie algebras.**

Definition 2.5.1. A twisted Lie algebra L is a twisted module together with a morphism of twisted modules $\beta : L \otimes L \to L$, called the bracket, which satisfies the traditional anticommutativity and Jacobi identities:

$$\beta + \beta \circ T = 0 \text{ in } \mathrm{Hom}_{R(\mathfrak{S})}(L \otimes L, L)$$

$$\beta\circ(\beta\otimes L)+\beta\circ(\beta\otimes L)\circ(2,3,1)_{\#}+\beta\circ(\beta\otimes L)\circ(2,3,1)_{\#}^2 = 0 \ \mathrm{Hom}_{R(\mathfrak{S})}(L\otimes L\otimes L, L)$$

where $(2,3,1)_{\#}$ acts on $L \otimes L \otimes L$ by $x \otimes y \otimes z \mapsto y \otimes z \otimes x$.

Let us be redundant and transcribe this definition on elements. As usual we write the bracket $\beta = [,]$ and the identities are written with explicit elements $u_i \in L_{p_i}$ for $i = 1,2,3$:

$$[u_1, u_2] = [u_2, u_1] \circ \mathcal{C}_{p_2,p_1}((2,1))$$

$$[[u_1,u_2],u_3]+[[u_2,u_3],u_1]\mathcal{C}_{p_2,p_3,p_1}((2,3,1))+[[u_3,u_1],u_2]\mathcal{C}_{p_3,p_1,p_2}((3,1,2)) = 0$$

As in the classical case we can define a Lie bracket on each twisted algebra A by $\beta = \mu - \mu \circ T$ or on elements $[x,y] = xy - yx\mathcal{C}_{q,p}((2,1))$ for x and y elements of A of respective degrees p and q.

We conclude here the reminder on generalities about twisted algebraic structures. It gives a convenient framework to understand the notations of the coming sections. The paper of Stover ([12]) continues with enveloping algebras and the Milnor-Moore theorem.

Actually the theorem of Milnor Moore also holds in the twisted context. Even if we shall need only part of the well-known results, let us recall some facts about primitive elements.

2.6. **Primitives in a twisted Hopf algebra.** If A is a twisted bialgebra, an element $a \in A$ is primitive if $\Delta(a) = a \otimes 1 + 1 \otimes a$. The set of primitives of A is a twisted sub-module of A, denoted by PA.

Let us mention two results about PA (cf. [12] Prop. 7.8 and 8.10).

Proposition 2.6.1. *Consider A as the twisted Lie algebra whith bracket canonically induced by the (associative) product of A. Then PA is a twisted Lie sub-algebra of A.*

Proposition 2.6.2. *If the Hopf algebra A is cocommutative, then the inclusion $PA \subset A$ induces an isomorphism of twisted Hopf algebras $UPA \cong A$.*

In the next section we wish to spread some light on various notions of free twisted objects. The most general one is defined by the usual process of adjunction (cf [12]). Barratt [2], much more restrictive, defines an explicit basis in degree 1. Finally we shall extend the definition of [2] to generators of any degree: for that we introduce the notion of twisted polynomials.

Let us now proceed and fix some ideas about free twisted objects.

3. Free twisted objects and twisted Lie polynomials

In this section we follow again Stover [12] and adapt the first chapter of Reutenauer's book [11] to the case of twisted structures.

First let us recall some basic definitions and properties of free monoids. Here no twisting occurs and we shall be brief.

3.1. **Words and free monoids.** Let X be a set, finite or infinite, and denote its elements by x or x_i, for i on some indexing set. A juxtaposition (or concatenation) of a finite number of ordered letters, e. g. $x_1 x_2 \dots x_n$, is called a word. The collection of all words generated by X, denoted by $W(X)$, comes with an obvious embedding of sets $\imath : X \to W(X)$. Moreover $W(X)$ admits a product, called the concatenation product, defined as in the following example: $(x_1 \dots x_n)(x'_1 \dots x'_{n'}) = x_1 \dots x_n x'_1 \dots x'_{n'}$. $W(X)$ with this product is a free monoid. This definition is justified by the following.

Proposition 3.1.1. *For any monoid M and any map of sets $f : X \to M$ there is a unique map of monoids $\overline{f} : W(X) \to M$ such that the following diagram in the category of sets commutes:*

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "\imath"'] & & M \\ & W(X) \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

3.2. **Definitions of free twisted objects and polynomials.** Let X be a graded set (each $x \in X$ is equipped with a positive integer $\mid x \mid$ called the degree) and R be a ring. The twisted free module over R generated by X is any twisted module isomorphic to $\oplus_{x\in X} xR(\mathfrak{S}_{|x|})$ and is denoted by $R(\mathfrak{S})(X)$. Again there is an obvious embedding of sets $\imath : X \to R(\mathfrak{S})(X)$.

Proposition 3.2.1. *For any twisted module M and any map of graded sets $f : X \to M$ there is a unique map of twisted module $\overline{f} : R(\mathfrak{S})(X) \to M$ such that the following diagram in the category of graded sets commutes:*

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "\imath"'] & & M \\ & R(\mathfrak{S})(X) \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

Proof. Given any element $x_1r_1 + \cdots + x_nr_n$, $x_i \in X, r_i \in R(\mathfrak{S})$, the commutation of the diagram implies that $\overline{f}(x_i) = f(x_i)$ and by linearity $\overline{f}(x_1r_1 + \cdots + x_nr_n) = f(x_1)r_1 + \cdots + f(x_n)r_n$. Thus $\overline{f}$, if existing, is unique. Moreover the preceding formula is precisely a definition of $\overline{f}$ once f is given.

□

Now let M be a twisted module over R. Let us denote by $M^{\otimes n}$ the twisted module given by the tensor product of n copies of M and by $T(M)$ the direct sum $\oplus_{n>1} M^{\otimes n}$ (see subsection 2.2 for the definition of the twisted tensor product). The associativity formula of subsection 2.2 defines a (product) map $M^{\otimes n} \otimes M^{\otimes m} \to M^{\otimes (n+m)}$ which by linearity extends to $T(M)$ and endows it with a structure of an associative twisted algebra. This is called the free twisted (associative) algebra generated by the twisted module M. There is an obvious embedding of twisted modules $\imath : M \to T(M)$. This terminology is justified by the following:

Proposition 3.2.2. *For any twisted (associative) algebra A and any map of twisted modules $f : M \to A$ there is a unique map of twisted algebras $\overline{f} : T(M) \to A$ such that the following diagram in the category of twisted modules commutes:*

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, "\wr"'] & & A \\ & T(M) \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

Proof. Given an element $m_1 \otimes \cdots \otimes m_i \otimes \sigma$ define $\overline{f}(m_1 \otimes \cdots \otimes m_i \otimes \sigma) = f(m_1) \otimes \cdots \otimes f(m_i) \otimes \sigma$. A straightforward inspection shows that $\overline{f}(m_1\sigma_1 \otimes \cdots \otimes m_i\sigma_i \otimes \sigma) = f(m_1)\sigma_1 \otimes \cdots \otimes f(m_i)\sigma_i \otimes \sigma = f(m_1) \otimes \cdots \otimes f(m_i)(\sigma_i \times \sigma_1 \times \cdots \times \sigma_i)\sigma$. This proves, first, that $\overline{f}$ is well-defined on $T(M)$ as a twisted module map and, secondly, that $\overline{f}$ is multiplicative. Moreover, and by definition, $\overline{f} = f$ on the twisted module M. This completes the proof. □

We briefly pause here to emphasize an important point we shall only use in the next subsection. Consider the map of twisted modules $\Delta : M \to T(M) \otimes T(M)$ given by $\Delta(m) = m \otimes 1 + 1 \otimes m$ and extend it to obtain a map of twisted algebras $\Delta : T(M) \to T(M) \otimes T(M)$. This process endows $T(M)$ with a structure of twisted bialgebra. Actually this bialgebra is connected; indeed it is easy to check that the anti-automorphism $S : T(M) \to T(M)$ defined by $S(m) = -m$ (just apply the universal property of proposition 3.2.2 to the algebra opposite to $T(M)$) satisfy the axioms of an antipode for $T(M)$. In other words we just defined the structure of twisted Hopf algebra for $T(M)$.

Now let us specialize to the free twisted module generated by a graded set X. Let us denote by $\mathcal{F}(X)$ the free twisted associative algebra $T(R(\mathfrak{S})(X))$. Combininig propositions 3.2.1 and 3.2.2 , we readily obtain

Proposition 3.2.3. *For any twisted associative algebra A and any map of graded sets $f : X \to A$ there is a unique map of twisted algebras $\overline{f} : \mathcal{F}(X) \to A$ such that the following diagram in the category of graded sets commutes:*

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "\wr"'] & & A \\ & \mathcal{F}(X) \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

We end this subsection by introducing polynomials in the twisted case. A typical element of $R(\mathfrak{S})(X))$ may be written as $\sum_{i\in I} x_i \circ \sigma_i$, for a finite indexing set I. Thus $\mathcal{F}(X)$ is linearily generated (i.e.as an $R(\mathfrak{S})$-module) by elements of the type $\otimes_{j\in J} x_j$ where J browses all finite tuples of elements of X. Such an element is also written $x_1 \dots x_j$ for a j-uple $(x_1, \dots, x_j)$ and is called a monomial of $\mathcal{F}(X)$. The collection of monomials is a linear basis for $\mathcal{F}(X)$. In the algebra $\mathcal{F}(X)$ the product of polynomials follows the rules of the product in a free twisted algebra edicted in subsection 2.2:

$$\begin{aligned}
& ((x_{1,1}\sigma_{1,1} \otimes \cdots \otimes x_{1,k}\sigma_{1,k})\tau_1 \times (x_{2,1}\sigma_{2,1} \otimes \cdots \otimes x_{2,l})\sigma_{2,l})\tau_2 \\
= \quad & ((x_{1,1}\sigma_{1,1} \otimes \cdots \otimes x_{1,k}\sigma_{1,k}) \otimes (x_{2,1}\sigma_{2,1} \otimes \cdots \otimes x_{2,l}\sigma_{2,l}))\tau_1 \times \tau_2 \\
= \quad & (x_{1,1} \otimes \cdots \otimes x_{1,k} \otimes x_{2,1} \otimes \cdots \otimes x_{2,l})(\sigma_{1,1} \times \cdots \times \sigma_{1,k} \times \sigma_{2,1} \times \cdots \times \sigma_{2,l})(\tau_1 \times \tau_2).
\end{aligned}$$

3.3. **Free twisted Lie algebras and Lie polynomials.** We refer here to Stover ([12]), specially for the proofs.

Consider a non-associative abstract operation on symbols and write it as a bracketting. Starting with a unique symbol - say x - the bracketting operation gives rise to an infinite set $\mathcal{N}(x)$ - the free non-asociative monoid generated by x. Given a twisted module M and an element b of $\mathcal{N}(x)$, we define $M^{\otimes b}$ as the twisted module $M^{\otimes \# b}$, where $\#b$ denotes the number of occurrences of x in b, and the twisted structure is similar to the twisted structure of the ordinary tensor product. The bracketting operation in the monoid $\mathcal{N}(x)$ induces an obvious bracketting operation $M^{\otimes b} \otimes M^{\otimes c} \to M^{\otimes (bc)}$. Let us define the twisted module $\mathcal{T}(M) = \oplus_{b\in\mathcal{N}(x)} M^{\otimes b}$. The bracketting operation just defined extends to $\mathcal{T}(M)$ by linearity. Call it β.

Define $\mathcal{I}(M)$ as the two sided twisted ideal of $\mathcal{T}(M)$ generated by the images of

$$\begin{aligned}
&\beta + \beta \circ (2,1) : \mathcal{T}(M) \times \mathcal{T}(M) \to \mathcal{T}(M) \\
&\beta \circ (\beta \times \mathcal{I}(M)) + \beta \circ (\beta \times \mathcal{I}(M))(2,3,1) + \beta \circ (\beta \times \mathcal{I}(M))(2,3,1)^2 : \\
&\mathcal{T}(M) \times \mathcal{T}(M) \times \mathcal{T}(M) \to \mathcal{T}(M)
\end{aligned}$$

The quotient $\mathcal{L}(M) = \mathcal{T}(M)/\mathcal{I}(M)$ is equipped with the map induced by β (denoted as usual by [,]) and is called the free twisted Lie algebra generated by M, denomination justified by the following proposition proved by Stover [12]. There is an obvious embedding of twisted modules $\imath : M \to \mathcal{L}(M)$.

Proposition 3.3.1. *For any twisted Lie algebra L and any map of twisted modules $f : M \to L$ there is a unique map of twisted Lie algebra $\overline{f} : \mathcal{L}(M) \to L$ such that the following diagram in the category of twisted modules commutes:*

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, "\imath"'] & & L \\ & \mathcal{L}(M) \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

Let us end this subsection with some lines about twisted universal enveloping algebras.

If L is a twisted Lie algebra, consider $T(L)$ the free (associative) twisted algebra generated by the twisted module L, with the linear embedding $\imath : L \to T(L)$. Now let IL be the two-sided twisted Lie ideal generated in $T(L)$ by elements of the form $[\imath(x), \imath(y)] - \imath[x, y]$.

The enveloping algebra of L is the quotient (associative) algebra $T(L)/I(L)$ and is denoted by UL. It satisfies the following :

Proposition 3.3.2. *For any Lie algebra L and any map of Lie algebras $f : L \to A$ there is a unique map of algebras $\overline{f} : UL \to A$ such that the following diagram in the category of sets commutes:*

$$\begin{tikzcd} L \arrow[rr, "f"] \arrow[dr, "\imath"'] & & A \\ & UL \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

And now we can phrase the twisted version of Milnor-Moore for free algebras given in [12], Prop. 7.4.

Proposition 3.3.3. *Let M be a twisted module. the twisted algebra map*

$$T(M) \to U\mathcal{L}(M)$$

induced by the composition of maps of twisted modules

$$M \to \mathcal{L}(M) \to U\mathcal{L}(M)$$

is an isomorphism.

As in the preceding subsection we can introduce Lie polynomials. Recall that a typical element of $R(\mathfrak{S})(X)$ may be written as $\sum_{i\in I} x_i \circ \sigma_i$, for an indexing set I and that a (non-commutative) polynomial in $\mathcal{F}(X)$ is a linear combination of elements such as $x_1\sigma_1 \otimes \cdots \otimes x_j\sigma_j$. By subsection 2.4 and proposition 3.3.1 we define an embedding of twisted Lie algebras: $\mathcal{L}(X) \subset \mathcal{F}(X)$. A polynomial in $\mathcal{F}(X)$ is called a Lie polynomial if it is in the image of $\mathcal{L}(X)$ by this embedding.

Remark. If we suppose that all elements of X are of degree 1, we recover Barratt's definition of a free twisted (associative) algebra and Lie algebra.

4. Lyndon words

Preliminary remark. One can ask - and we are grateful to the referee for his question - why we are limited to Lie algebras over free twisted modules. The reason rests on the next two sections. As the classical one (see [4]) our proof uses Lyndon words. Let us have an idea of the problem. Suppose M is defined on the rationals by two generators x and y of degree 2 and a relation $x(1+\epsilon) = y(1-\epsilon)$, where $\epsilon = (2, 1) \in \mathbb{Q}(\mathfrak{S}_2)$ (notice that $1-\epsilon$ and $1+\epsilon$ are zero divisors in $\mathbb{Q}(\mathfrak{S}_2)$ and the set of generators $\{x, y\}$ is minimal). Of course this relation induces further relations between all monomials in x and y and the fundamental theorem 4.2.2 is no more valid.

This section (and Section 5) follows the presentation of [4] in outline. We have now to handle carefully the twisted structures. We have precisely in mind that for an element u in a twisted Lie algebra the bracket $[\dots[u, u], \dots, u]]$ is not necessarily 0. So, when building a basis, we have to modify the classical definitions and to check properties again. Let us proceed for Lyndon words.

4.1. **Free twisted associative algebra context.**

First we fix a basis field $\mathbb{F}$ of characteristic 0. Let also X be a graded set; we denote its elements by x_i. Let us denote by $W(X)$ the set of words in X; the length of a word is the number of elements of X necessary to write it down by concatenation; conventionally 1 is the word of length 0. Write $\mathcal{F}(X)$ for the free associative twisted algebra generated by X (cf. Section 3); as an $\mathbb{F}(\mathfrak{S})$-module, $\mathcal{F}(X)$ admits $W(X)$ for basis. As usual the product in $\mathcal{F}(X)$ is denoted by simple juxtaposition "fg" and so the canonical Lie algebra structure on $\mathcal{F}(X)$ is given by $[f, g] = fg - gf\mathcal{C}_{|g|,|f|}((2, 1))$.

Finally let us write $\mathcal{L}(X)$ for the free twisted Lie algebra generated by X, which we consider as a Lie twisted subalgebra of $\mathcal{F}(X)$ with its canonical Lie algebra structure.

We now define Lyndon words of $\mathcal{F}(X)$ in various equivalent ways and examine how using them to obtain generators of $\mathcal{L}(X)$.

Let u, v, w be words (elements of $W(X)$) of strictly positive length such that $w = uv$. We say that u is a head of w and that v is a tail of w. We order words of $W(X)$ by lexicographic order and denote the order relation by $\geq$. In particular if $w \geq uv$, either the order is decided in u and $w \geq u$, or only in v and then u is a head of w.

Definition 4.1.1. A Lyndon word is a word that is strictly smaller than all its cyclic rearrangements or a power not less than 2 of a Lyndon word.

Remark. The preceding definition makes sense because it is recursive. Clearly all elements of X are Lyndon words (these are all Lyndon words of length 1 - like in the non-twisted case) and if $w = u^p, p \geq 2$ the length of u is strictly smaller that the length of w.

We fix now some notations. Let L (resp. L_n) denote all Lyndon words of $\mathcal{F}(X)$ (resp. of length n).

We say that a word $w = x_1 x_2 \dots x_k$ is not prime if there is some non-trivial circular permutation $\sigma \in \mathfrak{S}_k$ such that $w = x_{\sigma(1)} x_{\sigma(2)} \dots x_{\sigma(k)}$. In the opposite case we say that w is prime.

Proposition 4.1.2. *w is a Lyndon word if and only if*

1) *If w is prime, then w is strictly smaller than all its tails or*
2) *If w is not prime, then there exists a Lyndon word u such that $w = u^p$, $p > 1$.*

Proof. $\Leftarrow$

Suppose w is smaller than all its tails. Write $w = uv$, with u and v of strictly positive length. Then $w < v$ which implies $w < vu$. As v is a a tail of w, it means that w is strictly smaller than all its cyclic rearrangements.

$\Rightarrow$

Let $w = \alpha v$, with α and v of strictly positive length. Then $w < v\alpha$

(a) Either this inequality is decided in v and we are done.
(b) Or v is a head of w and $w = v\beta$. Then by hypoyhesis
   1) $w = \alpha v < \beta v$ and thus $\alpha < \beta$
   2) And vice-versa: $w = v\beta < v\alpha$ and thus $\beta < \alpha$

which shows that b) cannot happen.

□

Proposition 4.1.3. *w is a Lyndon word if and only if it has a factorization*

$$\textit{If } w \textit{ is prime: } w = w_1 w_2 \textit{ with } w_1, w_2 \in L \textit{ and } w_1 < w_2$$

or

$$\textit{If } w \textit{ is not prime} : w = u^p, p > 1 \ u \textit{ a prime Lyndon word.}$$

Moreover if w is prime and w_2 is the longest possible Lyndon word, w_1 and w_2 are prime.

Proof. $\Rightarrow$

Let $w = w_1 w_2$ with w_2 the longest Lyndon tail of w. We shall show first, that w_1 is strictly smaller than w_2 and secondly, that $w_1 \in L$, which means that the decomposition matches the request.

By Proposition 4.1.2 $w = w_1 w_2 < w_2$. Suppose $w_1 \geq w_2$; then $w_1 u \geq w_2$, for every word u, in particular $u = w_2$, which contradicts our hypothesis; so $w_1 < w_2$. Our first assertion holds.

Let us prove now that w_1 is a Lyndon word.

First examine the two possible cases.

A) w_1 is a prime word.

We use Proposition 4.1.2 again and show that w_1 is strictly smaller than all its tails. Decompose $w_1 = uv$, u and v of strictly positive length.

$w = uvw_2$ and our choice of w_2 implies that vw_2 cannot be a Lyndon word. So, by Proposition 4.1.2, there exists a decomposition $vw_2 = st$ with $t < vw_2$.

a) Either this inequality is decided in v : $v > t$. Going back to w we get $w = ust$ and $t > w = w_1 w_2 > w_1$ and we deduce $v > t > w_1$ as desired.

b) Or v is a head of t and we can write $t = vs$'; then $vw_2 = st = svs'$. In other words s' is a tail of w_2. Since w_2 is a Lyndon word :
i) Either $w_2 < s'$ and we derive

$$vw_2 > t = vs' > vw_2$$

which is a contradiction.
ii) Or $w_2 = u'^p, p > 1$, with u' a prime Lyndon word (equivalently : p maximal). If $s' = s''u'^k$ with s'' of length strictly positive, but smaller that the length of u'. Then s'' is a tail of u'. As u' is a prime Lyndon word : $u' < s''$.

Besides

$$vu'^p = vw_2 > t = vs''u'^k.$$

Since the length of s'' is strictly smaller than the length of u', this forces

$$u' > s''$$

in contradiction with the above assertion.

So the case $w_2 = u'^p$ cannot occur.

B) w_1 is not prime, say $w_1 = (uv)^p, p > 1$.

Then $w = (uv)^p w_2$. As w is a Lyndon word, our choice for w_2 implies that vw_2 is not a Lyndon word. Thus there exists a decomposition $vw_2 = st$, with $t < vw_2$.

a) Either this inequality is decided in v and $v > t$. Then

$$w = (uv)^{p-1} uvw_2 = (uv)^{p-1} ust$$

and, as w is a Lyndon word with tail t

$$t > (uv)^{p-1} ust > uv.$$

Thus

$$v > t > uv$$

which proves that uv is a Lyndon word.

Now

$$uv < (uv)^p < w_2$$

by the first part of the proof. Thus uvw_2 is a product of two Lyndon words uv and w_2 with $uv < w_2$. If we suppose recursively that the theorem holds in length smaller than the length of $\mid w \mid$, we conclude that uvw_2 is a Lyndon word, a contradiction with our hypothesis on w_2.

b) Or the inequality is not decided in v, and v is a head of t. Then we can reproduce the argument in A)b), because in this part of the proof we don't use that w is a Lyndon word, only the fact that w_2 is one.

So the study of the case B) proves that this case does not exist: w_1 is necessarily a prime word.

$\Leftarrow$

We use Proposition 4.1.2 once more and give ourselves a decomposition $w = uv$. We begin with the case where $v = w_2$ (and so $u = w_1$). By hypothesis $w_1 < w_2$. If this inequality is decided before the end of w_1, then $w_1\beta < w_2$ for every word β. If not, it means that w_1 is a head of w_2 and then we can write $w_2 = w_1\alpha$. Now w_2 is a Lyndon word and $w_2 < \alpha$ which implies $w = w_1w_2 < w_1\alpha = w_2$.

If v is shorter than w_2, then v is a tail w_2 and (always Proposition 4.1.2) $v > w_2 > w$.

If v is longer than w_2, w_2 is a tail v: $v = sw_2$ for some word s. Then s is a tail of w_1. Now w_1 is also a Lyndon word; thus $w_1 < s$ which implies $w = w_1w_2 < sw_2 = v$. This was to be proved. $\square$

Definition 4.1.4. A standard factorization of a Lyndon word w is a factorization of one of the two types:

i) $w = w_1w_2$ where w_1 and w_2 are Lyndon words, $w_1 < w_2$, with w_2 the longest word possible, or
ii) $w = u^p$, u a Lyndon word and $p > 1$, with the greatest p possible.

4.2. **Free twisted Lie algebra context.** In this section we explain how to use the Lyndon words to construct a basis of the free twisted Lie algebra.

Let us define a map $b : L \to \mathcal{L}(X)$. We start with $x \in X$: $b(x) = x \in \mathcal{L}(X)$. Then the definition is recursive: if $w = w_1w_2$ (factorization i) of definition 4.1.4) we set $b(w) = [b(w_1), b(w_2)]$; if $w = u^p$ (factorization ii) of definition 4.1.4), we set $b(w) = [[b(u), b(u)], \ldots, b(u)]$.

We are now ready to show how Lyndon words generate an independent set in $\mathcal{L}(X)$.

Proposition 4.2.1. *If w is a prime Lyndon word, then :*

$$b(w) = w + \sum_{v>w} va_v, \ \text{whith } a_v \in R(\mathfrak{S}).$$

If $w = u^p$, then :

$$b(w) = (b(u))^p(1 - \gamma_2)\ldots(1 - \gamma_p)$$

where γ_i is the permutation of $\mathcal{C}_{(i-1)|u|,|u|}((2,1))$ of $\mathfrak{S}_{i|u|}$.

Proof. We begin with the case $w = u^p$. By recursion it is enough to prove that $b(w) = b(u^{p-1})b(u)(1 - \gamma_p)$. Now $b(u^p) = [b(u^{p-1}), b(u)]$ by definition of b; then apply the definition of the twisted Lie bracket in $\mathcal{F}(X)$.

Let us now examine the prime case. Again we proceed recursively. So we have the standard factorization $w = w_1 w_2$ and by the hypothesis of recursion we can write when w_1 and w_2 are prime:

$$b(w) = w_1 w_2 - w_2 w_1 \mathcal{C}_{|w_1|,|w_2|}((2,1)) + \sum (v_1 v_2 - v_2 v_1 \mathcal{C}_{|v_1|,|v_2|}((2,1)))$$

where the sum is over all pairs (v_1, v_2) where v_i appears in the decomposition of w_i excepting the pair (w_1, w_2). So $v_1 v_2 > w_1 w_2$ because either $v_1 > w_1$ or if $v_1 = w_1$ then $v_2 > w_2$. Similarly $v_2 v_1 > w_2 w_1$; and $w_2 w_1 > w_1 w_2$ because $w_1 w_2 = w$ is a Lyndon word.

If $w_1 = u^p$ or $w_2 = v^q$, then the same argument holds.

□

The last discussion leads immediately to the fundamental result:

Theorem 4.2.2. *The polynomials $\{b(w)\}_{w \in L}$ are independant in $\mathcal{F}(X)$.*

We want now to prove that these polynomials are generating. As in the classical case the major tool is the Klyachko idempotent.

5. The Klyachko idempotent

We follow here the presentation of [9] and work in a bialgebra. We shall specialize to the Lie algebra in the next section.

Let A be a twisted bialgebra and $\mathbb{F}$ be a field of charactersitic 0, which countains a primitive nth root of the unity ω_n for any $n \geq 1$. Let $p_n : A \to A_n \hookrightarrow A$ be the projection of A onto its component of degree n (viewed as a morphism of $\mathrm{End}_{\mathbb{F}(\mathfrak{S})}(A)$) and define $p_C = p_{i_1} \star \cdots \star p_{i_l}$, where C denotes the l-uple of strictly positive integers $(i_1, \ldots, i_l)$; we shall also say that C is a composition of $(i_1 + \cdots + i_l)$. By definition C is finer than C' and write $C' \leq C$ if C' is obtained from C by substituting to a subset of consecutive entries of C (say $i_k, i_{k+1}, \ldots, i_{k+l}$, $1 \leq k \leq k+l \leq j$) their sum $(i_k + \cdots + i_{k+l})$; notice that this substitution does not change the total sum of all entries of C, which we call the weight - see below.

By inclusion exclusion we define elements r_C of $\mathrm{End}_{\mathbb{F}(\mathfrak{S})}(A)$ by the formula

$$p_C = \sum_{C' \leq C} r_{C'}.$$

More precisely, let $l(C)$ be the length - the number of entries - of C. Then (by Moebius inversion):

$$r_C = \sum_{C' \leq C} (-1)^{l(C') - l(C)} p_{C'}. \qquad (1)$$

For any l-uple $C = (i_1, \ldots, i_j)$ define its weight by $\mid C \mid = i_1 + \cdots + i_l$ and its major index by $maj(C) = (l-1)i_1 + (l-2)i_2 \cdots + i_{l-1}$. With this notation let us define:

Definition 5.0.3. The Klyachko idempotent - this denomination will be justified below - of order n is the morphism $\kappa_n \in \mathrm{End}_{\mathbb{F}(\mathfrak{S})}(A)$ given by the formula:

$$\kappa_n = \frac{1}{n} \sum_{|C|=n} \omega_n^{maj(C)} r_C$$

Theorem 5.0.4. *If A is a cocommutative, connected bialgebra, then κ_n maps A into the primitives of the bialgebra A.*

Proof. We reproduce the proof of [9] and use the short cut presented in [5]. A priori we have to pay attention to the action of $\mathfrak{S}$, in particular when dealing with tensor products.

Actually the general presentations by morphisms ([9]) veils the effective action of $\mathfrak{S}$: the abstract formulas for structure maps of the twisted bialgebra A do not involve permutations explicitly; they only appear when we want to make them explicit on elements of A.

We define $\mathrm{Endgr}(A) = \oplus_{n>0} \mathrm{End}_{\mathbb{F}(\mathfrak{S}_n)}(A_n)$. Let q be a variable; then $\mathrm{Endgr}(A)[[q]]$ makes sense. As the morphisms of $\mathrm{End}_{\mathbb{F}(\mathfrak{S})}(A)$ are of degree 0, there is a bijection between $\mathrm{End}(A)$ and $\mathrm{Endgr}(A)$ compatible with the action of $\mathbb{F}(\mathfrak{S}_n)$; so we can transfer the convolution product to $\mathrm{Endgr}(A)$. Define $P(q) = \sum_{n \geq 0} p_n q^n \in \mathrm{Endgr}(A)$. The infinite product

$$\kappa(q) = \cdots \star P(q^n) \star \cdots \star P(q) \star P(1)$$

is well-defined in $\mathrm{Endgr}(A)[[q]]$, because A is connected.

Observe that each element of $\mathrm{Endgr}(A)[[q]]$ has a unique expression as a sum $\sum_n f_n$, with $f_n \in \mathrm{End}(A_n[[q]])$. Like in [9] (after [5]); these elements can be easily deduced from the formula:

$$\kappa(q) = \sum_{n \geq 0} \frac{K_n(q)}{(q)_n}$$

with $(q)_n = (1-q) \dots (1-q^n)$ and $K_n(q) = \sum_{|C|=n} q^{maj(C)} r_C$. Notice that in the above formula n actually is the degree which is involved in $\mathrm{Endgr}(A)$

We extend the definition of pseudo-coproduct recalled in Section 2 and say that $f \in \mathrm{Endgr}(A)[[q]]$ admits the pseudo-coproduct $F \in \mathrm{Endgr}(A) \otimes \mathrm{Endgr}(A)[[q]]$ if $F \circ \delta = \delta \circ f$ where δ extends naturally to $A[[q]]$. Moreover there is a natural bijection (compatible with the action of the $\mathfrak{S}_n$) between $\mathrm{Endgr}(A)[[q]]$ and $\mathfrak{S}$-morphisms $A \to A[[q]]$ (similarly between $\mathrm{Endgr}(A) \otimes_{\mathbb{F}} \mathrm{Endgr}(A)[[q]]$ and morphisms $A \otimes_{\mathbb{F}} A \to A \otimes_{\mathbb{F}} A[[q]]$. We systematically identify $\mathrm{Endgr}(A) \otimes_{\mathbb{F}[[q]]} \mathrm{Endgr}(A)[[q]]$ with$(\mathrm{Endgr}(A) \otimes_{\mathbb{F}} \mathrm{Endgr}(A))[[q]]$. Granting this, when $f, g \in \mathrm{Endgr}(A)[[q]]$ we consider $f \otimes g$ as an element of $(\mathrm{Endgr}(A) \otimes_{\mathbb{F}} \mathrm{Endgr}(A))[[q]]$. With all these conventions Theorem 5.0.8 of [1] applies, since we assumed A to be cocommutative.

We check that $\sum_{i+j=n} p_i \otimes p_j \circ \delta = \delta \circ p_n$, i. e. $\sum_{i+j=n} p_i \otimes p_j$ is a pseudo-coproduct for p_n (this is general; if $f = \sum f_n$, $f \otimes f$ is a pseudo-coproduct for f if and only if $\sum_{i+j=n} f_i \otimes f_j$ is a pseudo-coproduct for f_n).

This is equivalent to say that $P(q) \otimes P(q)$ is a pseudo-coproduct for $P(q)$ (the same is true for $P(q^n)$ for any $n > 0$). Then, applying Theorem 5.0.8 of [1], we deduce that $\kappa(q) \otimes \kappa(q)$ is a pseudo-coproduct for $\kappa(q)$. By the above result, it means that $\sum_{i+j=n} \frac{K_i(q)}{(q)_i} \otimes \frac{K_j(q)}{(q)_j}$ is a pseudo-coproduct for $\frac{K_n(q)}{(q)_n}$, or equivalently $\sum_{i+j=n} \frac{(q)_n}{(q)_i(q)_j} K_i(q) \otimes K_j(q)$ is a pseudo-coproduct for $K_n(q)$. The polynomials $\frac{(q)_n}{(q)_i(q)_j}$ vanish for $q = \omega_n$, except the cases where $i = 0$ or $j = 0$ (in both cases they are equal to 1). This means that $K_n(\omega_n) = n\kappa_n$ is pseudo-primitive and proves the theorem.

□

Corollary 5.0.5. *If A is a cocommutative, connected bialgebra, then κ_n is an idempotent.*

Proof. For sake of completenes, we reproduce the proof of [4]. Here there is no changes introduced by the action of $\mathfrak{S}$.

First notice that the coproduct δ of the bialgebra A preserves the degree; therefore p_C is 0 on all elements of A of degree non equal to the length of C (just consider the coassociativity of the coproduct - which implies the associativity of the convolution). So, by the previous theorem and since A - a cocommutative and connected bialgebra - is generated by its primitive elements (proposition 2.6.2), it is enough to prove that $\kappa_n(a) = a$ for any primitive element $a \in A$; by the preceding remark there is no restriction to suppose $\mid a \mid= n$. As a is primitive $p_i \star p_j(a) = 0$, and $p_C(a) \neq 0$ only if C is of length 1. Equation (1) implies that $r_C(a) = (-1)^{l(C)-1}a$, for each C of weight n. Thus:

$$n\kappa_n(a) = \sum_{|C|=n} \omega_n^{maj(C)}(-1)^{l(C)-1}a.$$

Now there is classical bijection between compositions of n and subsets of $\{1, \ldots, n-1\}$, sending $S = (i_1, \ldots, i_l)$ onto $S = \{i_1, i_1+i_2, \ldots, i_1+\cdots+i_{l-1}\}$. The cardinality of S is $l(C) - 1$ and we define maj $(S) = \sum_{i \in S} i =$ maj (C). With these notations

$$\begin{aligned}
n\kappa_n(a) &= \sum_{S \subset \{1,\ldots,n-1\}} \omega_n^{maj(S)}(-1)^{\mathrm{card}(S)}a \\
&= \sum_{1 \leq i_1 < \cdots < i_r \leq n-1} \omega_n^{i_1+\cdots+i_r}(-1)^r a \\
&= \prod_{1 \leq i \leq n-1\}} (1 - \omega_n^i)a \\
&= (1 + 1 + \cdots + 1)a = na
\end{aligned}$$

since ω_n is a primitive n-root of the unity. □

6. The Lyndon-Hall basis

This section tells how to use the Klyachko idempotent for proving that the Lyndon words are generating.

We proved in Corollary 5.0.5 that κ_n is the identity on primitives of the bialgebra $\mathcal{F}(X)$. Moreover κ_n maps $\mathcal{F}(X)$ into its primitive elements. That recalled, by the Theorem of Milnor-Moore 3.3.3, we conclude $\kappa_n(\mathcal{F}(X)) = \mathcal{L}(X)$.

In theorem 3.2.2 we proved that the set L of Lyndon words determines a minimal set of independant elements in $\mathcal{L}(X)$. In this section we want to prove that this set is generating (actually this is directly related to the fact that, by definition, L forms a set of representatives of all circular rearrangements classes of words of $W(X)$). Let us see that.

To this purpose we shall use the Klyachko idempotent κ_n. The following theorem tells us that κ_n does not discriminate between all circular rearrangements of a same word. This property is given by the study of the kernel of the Klyachko invariant. For this part we work in the general context of a connected cocommutative bialgebra A.

Theorem 6.0.6. *The kernel of κ_n restricted to A_n is spanned by the elements of the form $ab - \omega^{|b|} ba\mathcal{C}_{|b|,|a|}((2,1))$.*

Proof. We directly use the proofs of Theorem 16, Lemma 14 and Corollary 15 given in [9]. The proof of theorem 16 explicitly rests on the fact that primitive must be generating in A; hence the hypothesis on A.

First recall the principle of the proof. We examine a word $a_1a_2\dots a_p$ with total degree $\mid a_1 \mid + \mid a_2 \mid + \dots + \mid a_p \mid = n$, its image $\kappa_n(a_1a_2\dots a_p)$ and the circular permutation $a_pa_1\dots a_{p-1}$ and its image $\kappa_n(a_pa_1\dots a_{p-1})$. Both images are linear combinations of words obtained by permutations of $a_1a_2\dots a_p$. Then, focus our attention to such a word w. In the classical case one proves that the coefficient of w in $\kappa_n(a_pa_1\dots a_{p-1})$ is equal to the coefficient of the same w in $\kappa_n(a_1a_2\dots a_p)$ multiplied by $\omega_n^{|a_p|}$.

Now we want to extend this classical case (the basis ring is a field $\mathbb{F}$ of characteristic 0 - possibly extended by primitive roots of unity) to the twisted case : the basis ring is the group ring $\mathbb{F}(\mathfrak{S})$. The coefficient of the word w mentionned in the preceding paragraph results from two distinct processes. First, a linear combination in $\mathbb{F}$ of coefficients of the form $\omega_n^{maj(C)}$ which appear in the definition of κ_n; notice that if, in the classical case, we calculate $p_{|a_1|} \star p_{|a_2|} \star \dots \star p_{|a_p|}(a_1a_2\dots a_p)$, where the $a_1, a_2, \dots, a_p$ are primitive, we obtain a combination of words obtained by some permutations of the word $a_1a_2\dots a_p$ all coefficient equal to 1. Secondly, the action of the group of permutations. It is generated by a repeated application of the following formula : $\delta(a_1a_2) = a_1a_2 \otimes 1 + a_1 \otimes a_2 + a_2 \otimes a_1\mathcal{C}_{|a_2|,|a_1|}((2,1)) + 1 \otimes a_1a_2$. As a consequence, if in $p_{|a_1|} \star p_{|a_2|} \dots \star p_{|a_p|}(a_1a_2\dots a_p)$ appears a word $a_{\sigma(1)}a_{\sigma(2)}\dots a_{\sigma(p)}$ for some permutation σ its coefficient in $\mathbb{F}(\mathfrak{S})$ is $\mathcal{C}_{|a_{\sigma(1)}|,|a_{\sigma(2)}|,\dots,|a_{\sigma(p)}|}$.

So if we determine the coefficient of $w = a_{\sigma(1)}a_{\sigma(2)}\dots a_{\sigma}(p)$ in $\kappa_n(a_1a_2\dots a_p)$ we obtain the coefficient given in [9], multiplied by $\mathcal{C}_{|a_{\sigma(1)}|,|a_{\sigma(2)}|,|\dots a_{\sigma(p)}|}(\sigma)$.

Similarly if we determine the coefficient of $w = a_{\sigma(1)}a_{\sigma(2)}\dots a_{\sigma(p)}$ in $\kappa_n(a_pa_1\dots a_{p-1})(-\omega_n^{|a_p|})\mathcal{C}_{(|a_p|,|a_1|+\dots a_{p-1}|)}((2,1))$ we obtain the coefficient given in [9] multiplied by $\mathcal{C}_{|a_{\sigma(1)}|,|a_{\sigma(2)}|,|\cdots|a_{\sigma(p)}|}(\sigma)$, the same permutation as above (indeed a permutation is given by its image and in our case by the word w).

In conclusion, the proof of [9] still works in the twisted case.

□

We now go back to the case of $A = \mathcal{F}(X)$.

First we remark that the free twisted bialgebra on X can be generated on $\mathbb{F}(\mathfrak{S})$ by the reunion of all $\{b(w)\}_{w\in L}$ and the non-trivial circular rearrangements of all w in L :

Lemma 6.0.7. *Let $< L_n >$ be the twisted module generated by L_n in $\mathcal{F}(X)$, B_n its image by the linear extension of $b : L \to \mathcal{L}(X) \subset \mathcal{F}(X)$ and K_n the kernel of the Klyachko idempotent $\kappa_n : \mathcal{F}(X)_n \to \mathcal{L}(X)_n \subset \mathcal{F}(X)_n$. Then there is an isomorphism between $< L_n > \oplus K_n$ and $B_n \oplus K_n$.*

Proof. Look at the decomposition given by Theorem 4.2.2. Consider the basis of B_n consisting in all $b(w)$, $w \in L_n$ and order it lexicographically. Similarly we consider the basis of $< L_n >$ consisting in all w, $w \in L_n$ again ordered lexicographically. Choose some basis for K_n. Then Theorem 4.2.2 implies that the matrix giving the basis of $B_n \oplus K_n$ in the basis of $< L_n > \oplus K_n$ is a triangular matrix with 1 at each spot of the diagonal. This proves the lemma. □

Remark. If we recall that the Lyndon words are the representatives of all circular rearrangement classes of $W(X)$, we see that $< L_n > \oplus K_n = \mathcal{F}(X)$.

We can now prove the following sequence of inclusions:

$$\begin{aligned}
\mathcal{L}(X)_n \supseteq B_n &= \kappa_n(B_n) \\
&= \kappa_n(B_n \oplus K_n) \text{ by definition of } K_n \\
&= \kappa_n(< L_n > \oplus K_n) \text{ by Lemma 6.0.7} \\
&= \kappa_n(\mathcal{F}(X)) \text{ by the above remark} \\
&= \mathcal{L}(X)_n \text{ by Milnor Moore, Proposition 3.3.3.}
\end{aligned}$$

So we can state:

Theorem 6.0.8. *As a twisted module the free (twisted) Lie algebra is generated by the Lie elements associated to all Lyndon words.*

Combining this with Theorem 4.2.2 we obtain our main result:

Theorem 6.0.9. *The set of Lie elements associated to all Lyndon words is minimal and generating for the free twisted Lie algebra.*

To conclude with, we now return to [2] and specify:

(i) each $b(w)$, w a prime Lyndon word, generates submodule isomorphic to $\mathbb{F}(\mathfrak{S}_{|w|})$ in $\mathcal{L}(X)$.

(ii) each $b(w)$, $w = u^p$, $p > 1$ and u a prime Lyndon word, generates submodule isomorphic to $\mathbb{F}(\mathfrak{S}_{|w|})/I_{p,|u|}$ in $\mathcal{L}(X)$, where $I_{p,|u|}$ is the annihilator of $(1-\gamma_2)\dots(1-\gamma_p)$ (cf. Proposition 4.2.1).

References

[1] Aubry, M., Twisted Lie algebra and idempotent of Dynkin, to appear in Séminaire Lotharingien de Combinatoire, vol. 62.

[2] Barratt, M. G., Twisted Lie algebras. Geometric applications of homotopy theory (Proc. Conf., Evanston, Ill., 1977), II, pp. 9–15, Lecture Notes in Math., 658, Springer, Berlin, 1978.

[3] Fresse, B., Koszul duality of operads and homology of partition posets. Homotopy theory: relations with algebraic geometry, group cohomology, and algebraic K-theory, 115–215, Contemp. Math., 346, Amer. Math. Soc., Providence, RI, 2004.

[4] Garsia, A. M. Combinatorics of the free Lie algebra and the symmetric group. *Analysis, et cetera*, 309–382, Academic Press, Boston, MA, 1990

[5] Gelfand, I. M.; Krob, D.; Lascoux, A.; Leclerc, Bernard; Retakh, V. S.; Thibon, J.-Y. Noncommutative symmetric functions.*Adv. Math.* **112** (1995), no. 2, 218–348..

[6] Joyal, A., Foncteurs analytiques et espèces de structures. Combinatoire énumérative (Montréal, Qué., 1985/Québec, Que., 1985), 126–159, Lecture Notes in Math., 1234, Springer, Berlin, 1986.

[7] Livernet, M.; Patras, F., Lie theory for Hopf operads, J. Algebra 319 (2008), no. 12, 4899–4920

[8] Markl, M.; Shnider, S.; Stasheff, J. Operads in algebra, topology and physics. Mathematical Surveys and Monographs, 96. American Mathematical Society, Providence, RI, 2002. x+349 pp.

[9] Patras, F.; Reutenauer, C., On Dynkin and Klyachko idempotents in graded bialgebras, Special issue in memory of Rodica Simion, *Adv. in Appl. Math.* **28** (2002), no. 3-4, 560–579.

[10] Patras, F.; Reutenauer, C., On descent algebras and twisted bialgebras. Mosc. Math. J. 4 (2004), no. 1, 199–216, 311.

[11] Reutenauer, C., Free Lie algebras. London Mathematical Society Monographs. New Series, 7. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1993. xviii+269 pp.

[12] Stover, C. R., The equivalence of certain categories of twisted Lie and Hopf algebras over a commutative ring *J. Pure Appl. Algebra* **86** (1993), no. 3, 289–326.

E-mail address: `aubry@math.unice.fr`

Laboratoire de Mathématiques Jean-Alexandre Dieudonné UMR CNRS n° 6621, Université de Nice, Parc Valrose, 06108 Nice cedex 02, France